Archivage des données
Plan de Reprise d'Activité

Table des matières

1 Introduction.

Les données de votre entreprise sont le bien le plus précieux qu'elle possède. Ces données sont l'actif le plus important sans aucune commune mesure avec le reste.

Imaginez que suite à un sinistre, la totalité de votre entreprise soit détruite, vous pourrez tout remplacer en le rachetant, mais vous ne pourrez jamais racheter vos données. Si elles ont disparu, elles le sont à jamais et ce quelque soit le montant que vous puissiez être prêt à débourser.

Qu'il s'agisse d'une erreur humaine, d'une panne système, d'un piratage ou d'une cause extérieure (incendie, inondation ...), perdre ses données constitue un des plus grand risque pour l'entreprise. Il est donc indispensable de les protéger et de les conserver bien à l'abri.

Par ailleurs, la loi impose aux chefs d'entreprises d'être en mesure de présenter au législateur différents documents qui se doivent donc d'être sauvegardés et archivés.

Ces lois vous imposent, de facto, de mettre en place les dispositifs de sauvegarde de vos données et notamment vos données légales. Ne pas mettre en place ce type de dispositif vous expose à des sanctions plus ou moins lourdes en cas de non-respect des règles définies par le législateur. Et ce, bien que la sauvegarde informatique en entreprise ne soit pas à proprement parler définie par la loi, l'archivage des données est, elle, une obligation légale. Si pour une raison quelconque, des données de votre entreprise se perdent et que vous n'aviez pas procédé à une sauvegarde, vous pouvez faire l'objet de poursuites pénales et votre entreprise peut connaître des dommages importants.

Il est donc indispensable qu'il existe, dans votre entreprise, un système de sauvegarde et d'archivage des données informatiques (disque dur, serveur externe, cloud, etc) afin de vous prémunir des pertes de données ou des sanctions administratives.

Ce document présente donc les choses importantes à savoir en matière d'archivage ou de sauvegarde ainsi que les solutions existantes et disponibles sur le marché.

2 Différence entre Sauvegarde et Archivage.

Sauvegarde (en anglais Back-up) :

Une sauvegarde correspond à une copie en masse des données, des applications ou documents sous toute forme numérique qui peuvent être utilisées pour restaurer les originaux dans le cas où ces derniers seraient endommagés ou perdus. La sauvegarde est utilisée en cas d'erreur humaine ou de problème technique. La sauvegarde est au final une copie des données.

Archivage :

Un archivage correspond à un ou plusieurs enregistrements de données, spécialement triées et sélectionnées pour une conservation dans le temps avec possibilité d'y accéder ultérieurement soit pour des raisons légales, soit pour le réutiliser. Avec l'archivage on prévoit de retrouver de manière logique et rapide les documents originaux déplacés de leurs emplacements de stockage initiaux et archivées à un autre endroit.

3 Sauvegarde ou archivage : De multiples enjeux.

Les enjeux induits par l'archivage et la sauvegarde en entreprise sont multiples :

Enjeu légal et juridique :

Légal parce que le législateur vous impose de conserver, a minima, vos documents légaux (factures, déclarations fiscales diverses er variées, contrats, …) … mais également juridique parce qu'en cas de contentieux, le système d'archivage électronique doit permettre de retrouver les pièces requises dans les délais impartis, d'autant que souvent ces documents seront certainement des éléments de preuve.

Autre aspect juridique : favoriser et informer des modalités d'accès à l'information de vos collaborateurs tout en respectant les droits d'accès établis.

Enjeu stratégique et organisationnel :

Décider quelles données doivent être conservées, en dehors des aspects purement obligatoires. Les organiser pour mieux les réutiliser ou les retrouver sur demande. Une entreprise se doit d'optimiser la structuration de ses données afin d'en faciliter la gestion, de maîtriser la redondance de l'information et de détruire les données inutiles ou périmées qui alourdissent le système.

Enjeu technologique.

Parce qu'il faudra bien choisir une solution technologique à la fois pérenne, fiable et capable d'absorber une augmentation des volumes de données à archiver (il est assez communément convenu qu'une PME double le volume de ses données chaque année).

4 Enjeu juridique : Que dit la loi ?

Pour les entreprises :

L' article 34 de la loi du 6 janvier 1978 du Code Pénal stipule que « Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».

La violation de cet article 34 est lourdement sanctionnée pénalement par l'article 226-17 du code pénal à (inventaire non exhaustif des sanctions prévues par la loi):

- Pour les données concernant la fiscalité : Majoration allant de 10 à 40% selon l'article 1728 du code général des impôts.
- Dans le cas d'un contrôle fiscal, le non accès aux documents par les agents des impôts est sanctionné par une amende de 25 000 euros doublée de 6 mois de prison en cas de récidive.
- La sauvegarde des données personnelles est soumise à une obligation de sécurité qui doit être garantie par le chef d'entreprise. Si cette obligation n'est pas respectée, l'amende peut atteindre 300 000 euros et être accompagnée de 5 ans de prison.
- Une amende de 150 euros est prévue si le chef d'entreprise ne peut produire les documents dans le respect des délais impartis.

Pour les collectivités :

Dans le cadre du décret N° 2010-112 du 2 février 2010, dit décret RGS (Référentiel général de Sécurité), un ensemble de règles de sécurité est défini pour la gestion de la sécurité de l'information qui s'applique aux autorités administratives. Ces règles sont plus ou moins drastiques selon plusieurs niveaux de « force sécuritaire » : une, deux ou trois étoiles (*, **, ***).

Quel que soit ce niveau la sauvegarde hors site des données est toujours recommandée. Elle est obligatoire dès le niveau **. Chaque collectivité doit mettre en œuvre une politique de sauvegarde et d'archivage (équipes à mobiliser, moyens nécessaires, procédures de reprise, …).

Dans tous les cas :

1. Il est important de définir la mise en place de l'organisation adéquate, les tests des procédures de secours, les données nécessaires à la reprise de l'activité, les moyens de récupérer les données à travers un site de secours ou une restauration de sauvegarde, les procédures de fonctionnement en mode dégradé.

2. Les moyens mis en œuvre pour sauvegarder et archiver ces données doivent être identifiés. Les procédures de sauvegarde et d'archivage doivent permettre de posséder l'information nécessaire en cas de besoin de restauration, notamment dans le cas de ruptures de services nécessitant le déclenchement du Plan de Reprise d'Activité, de satisfaire les contraintes légales et réglementaires sur la conservation des données, de définir les personnes pouvant accéder à ces informations, d'établir la fréquence de sauvegarde de ces données, de définir les types de données à sauvegarder, de décrire les procédures permettant de restaurer des données, de décrire les procédures d'accès et de récupération des archives, de déterminer les équipes à mobiliser en cas de telles demandes.

Attention vous ne pouvez pas tout sauvegarder sans en informer vos salariés, comme la CNIL le prévoit dans un document sur la surveillance des salariés sur le lieu de travail (https://www.cnil.fr/sites/default/files/typo/document/Guide_employeurs_salaries.pdf.pdf)

Ainsi vous devez informer vos salariés sur :

- Les zones sauvegardées.
- La durée de conservation des sauvegardes.
- Les personnes ayant accès aux sauvegardes.

5 Enjeu stratégique : Quelles données sauvegarder ?

Bien sûr, et a minima, les premières données à sauvegarder sont les données légales de l'entreprise, celles imposées par la législation (factures, Déclarations fiscales, RH …).

Ensuite il est indispensable, en fonction de l'organisation et la taille de l'entreprise, de déterminer quelles données il faut sauvegarder. En tout état de cause pour établir la liste des documents à conserver et leur durée, il vous sera certainement indispensable de constituer un groupe de travail pluridisciplinaire composé de personnes provenant du service juridique, de la direction informatique, de la direction achats, des archives ou de la documentation.

Liste non exhaustive des documents légaux à conserver.

Les documents concernant la gestion du personnel :

bulletins de paie, cartes de pointage, doubles des certificats de travail, soldes de tout compte, récapitulatif de charges sociales, etc.

Les documents commerciaux :

contrats commerciaux, commandes clients, commandes fournisseurs, dossiers clients, correspondance commerciale etc.

Les documents et pièces comptables :

livre comptable, bilans, comptes de résultats, comptes et journaux auxiliaires, inventaire, grand livre comptable etc.

contrats d'acquisition et de cession, factures clients et fournisseurs, bons de commande, justificatif de TVA etc.

Les documents bancaires :

ordres de virement, relevés trimestriels, avis de débit et de crédit etc.

Les documents sociaux :

registre des titres nominatifs, comptes sociaux, comptes d'exploitation, Procès verbaux des délibérations du Conseil d'administration, rapports des commissaires aux comptes etc.

Durée légale de la conservation des documents.

En annexe 1 vous trouverez, par type de document, les durées de conservation minimales imposées par la loi.

Autres données.

« Least but not last », il vous reviendra et à vos équipes de définir et lister quelles autres données sont indispensables à sauvegarder pour votre entreprise.

6 Enjeu technologique : Elaborer un cahier des charges.

Pour conserver toutes ces données, la mise en place d'une solution de sauvegarde/archivage informatique devient une question technique. Il convient donc d'élaborer un cahier des charges techniques qui permettra in fine de choisir, et la meilleure solution de support, et le meilleur prestataire.

Pour établir ce cahier des charges il apparaît donc nécessaire de procéder de la façon suivante :

1 - Etablir la liste exhaustive de toutes les données à sauvegarder et/ou archiver.

2 - Pour chaque groupe de données :

- Evaluer sa criticité (Légale, Indispensable, Important …),
- Définir leur durée de vie,
- Evaluer leur volume en Go,
- Définir la fréquence nécessaire de sauvegarde/archivage.

3 – Choisir les supports d'enregistrement et leurs localisations .

- Disques durs, clefs USB, serveurs,
- Cloud,
- En interne ou en externe,
- Par soi-même ou via un prestataire.

Bien évidemment c'est souvent la criticité, la durée de vie et le volume qui seront les éléments déterminants des choix qui seront faits. L'autre aspect déterminant réside dans le choix d'effectuer ses sauvegardes sur des supports internes ou externes à l'entreprise.

Nous ne saurions que trop recommander d'avoir recours aux deux (via un prestataire ou non). En effet, si l'on peut être rassuré par le fait que ses données soient hébergées à l'intérieur de l'entreprise, cette solution ne protège pas d'un sinistre (incendie par exemple) qui détruirait les machines et les sauvegardes. Dans le même ordre d'idée, le monde de l'entreprise ne compte-t-il pas un nombre incalculable de collaborateurs qui se sont fait voler leurs sacoches ordinateurs … et que, très consciencieux faisaient des sauvegardes régulières. Cependant leurs disques de sauvegarde étaient dans la sacoche qui leur a été volée !

Le recours à des sauvegardes internes et externes apparaît donc indispensable.

Impact du volume dans le choix d'une solution.

Le volume des données a des impacts sur plusieurs aspects des choix de solutions de sauvegarde : le support, la fréquence et la durée.

Si les données ne sont pas volumineuses, il est fort probable que le temps nécessaire à l'exécution de la sauvegarde soit assez court. D'autre part, elle n'exigera pas un support de grande capacité. Dans ce cas des disques durs externes ou des supports type DVD/clefs USB peuvent convenir.

Dans le cas de données volumineuses, non seulement il faudra s'assurer que

1. Les supports ont une taille suffisante pour enregistrer les données,
2. Qu'ils ont également une taille suffisante pour accueillir la croissance du volume de données,
3. Que le temps de sauvegarde n'est pas trop long (ex : Sauvegarde quotidienne qui dure 25 heures).

7 Solutions existantes.

Les solutions existantes sont multiples mais comme déjà indiqué, il y a lieu de multiplier les systèmes de sauvegarde et quelque soit le support, envisager des sauvegardes locales et des sauvegardes distantes.

Serveur de backup.

Les systèmes locaux sont multiples (DVD, disques externes, clefs USB) et les serveurs de back-up. Les serveurs de back-up sont intégrés dans le réseau informatique de l'entreprise et peuvent être de 2 types NAS (Network Attached Storage) ou SAN (Storage Area Network). De plus, au sein d'un serveur, il est possible de configurer ses disques en RAID pour les serveurs compatibles. Cela permet une sécurisation des données accrue tout en conservant un espace de stockage important et une vitesse de transmission des données qui n'est en aucun cas ralentie.

Il est recommandé de recourir à des dispositifs de sauvegardes automatisés sans aucune intervention humaine.

Sauvegarde en ligne (cloud).

La sauvegarde en ligne (cloud computing) est un bon moyen de protéger vos données, puisqu'elles seront ainsi stockées à l'extérieure de l'entreprise, vous protégeant ainsi contre tout incident qui pourrait survenir localement.

Dans le cas de sauvegardes distantes, il faut multiplier les sauvegardes sur deux, voire trois, sites. La plupart des solutions du marché sont automatisées, sécurisées et très souvent encryptées.

Choisir le site qui hébergera vos données n'est pas une décision à prendre à la légère. Certaines plates-formes ne sont pas fiables ou peu sécurisées. Préférez l'utilisation de sites de confiance ou proches de votre entreprise afin de pouvoir visiter les locaux et discuter directement avec le prestataire.

Nous vous rappelons que, en cas de perte de ses données, la responsabilité de l'entreprise et donc de son gérant peut-être engagée, pour faute ou non-respect des obligations légales listées précédemment.

8 Plan de reprise d'activité (PRA).

Toute entreprise se doit de mettre en place un plan de reprise d'activité. Malheureusement, il apparaît trop souvent que ces plans ne sont pas mis en place parce que jugés trop consommateur de temps ou simplement parce que l'on ne sait pas comment s'y prendre.

Voici une revue rapide pour vous aider à mettre en place cet indispensable Plan de reprise d'activité.

1. Impliquez vos employés dans cette réflexion, brainstormez et mettez en place des scénarios.
2. Assurez-vous que les documents et les données critiques sont également sauvegardées et archivées sur un site distant (pas dans les locaux de l'entreprise)
3. Faites en sorte de pouvoir accéder à vos données et documents si vous ne pouvez plus entrer dans vos locaux.
4. Faites de même avec les communications entrantes de vos clients (comment peuvent-ils vous joindre).
5. Nommer un responsable chargé de mettre en place, de surveiller et de régulièrement vérifier que toutes les procédures d'archivage, sauvegarde et reprise fonctionne.
6. Prévoyez des locaux de regroupement de vos employés et de vos activités en cas de sinistre
7. Vérifiez et remettez en cause régulièrement toutes les urgences/désastres/sinistres qui pourraient arriver.
8. Faites des plan de reprise « test » régulièrement. Mettez à jour les consignes dans le document décrivant le plan de reprise.
9. Diffusez l'information à toute l'entreprise. Mettez une copie du plan de reprise à l'abri et en sécurité (Il fait partie des données critiques).

Il arrivera forcément un jour où vous serez confronté à ce type d'événement et seule une préparation rigoureuse et suivie vous permettra de limiter les dégâts à ce qui est, rappelons-le encore, l'actif le plus précieux de votre entreprise : Ses données.

Comme nous l'écrivions en Introduction : « Vous ne pourrez jamais racheter vos données. Si elles ont disparu, elles le sont à jamais et ce quelque soit le montant que vous puissiez être prêt à débourser ».

9 Les étapes d'un PRA.

Il est communément admis par les spécialistes qu'un PRA se construit en 9 étapes, décrites ci-après. A noter qu'il existe des prestataires spécialisés qui peuvent vous assister pour définir et mettre en œuvre un PRA efficace. Si l'évaluation financière faite à l'étape 3 ci-dessous est importante, il ne serait que trop recommandé de faire appel à ces spécialistes.

Etape 1 : Impliquer la Direction Générale

Pour mettre en place un PRA efficace, la responsabilité globale du plan doit dépendre nécessairement de la direction générale. Celle-ci sera responsable de coordonner le PRA, nommer les personnes responsables, allouer les budgets nécessaires et assurer sa diffusion et son efficacité dans l'entreprise.

Etape 2 : Constituer une équipe chargée de rédiger le PRA.

Cette étape consiste à créer un groupe de travail comprenant des représentants fonctionnels de l'entreprise associés à la DSI. Cette équipe sera chargée de rédiger le PRA, ses procédures et sera responsable de sa mise en œuvre.

Etape 3 : Evaluer les risques.

La première tâche de l'équipe sera de lister et d'analyser les risques potentiels (incidents, menaces, sinistres potentiels) ainsi que les impacts possibles sur l'organisation. La protection des données et des documents critiques. A ce stade, il faut absolument tout considérer :

- Les sinistres liés à des causes externes (incendies, inondations, tremblements de terre, attentats, cambriolages …)
- Les sinistres liés à des causes internes (destruction de données volontaire ou involontaire par un membre du personnel, introduction volontaire ou involontaire de virus …

Il faut très nettement raisonner en envisageant les pires scenarios en fonction de la situation particulière de chaque entreprise.

A ce stade faites une estimation financière de la perte de vos données et documents critiques. Cela permettra à la Direction Générale de mettre les moyens adéquats en fonction des montants annoncés.

Etape 4 : Définir les priorités.

Les priorités doivent se définir par service et par organisation. Selon les problématiques de chacune, la tâche consiste à lister les éléments essentiels, importants, non importants.

Etape 5 : Déterminer les stratégies de reprise et de récupération des données.

Cette étape est souvent la tâche des informaticiens car il s'agit de considérer et dévaluer les matériels informatiques et logiciels, les télécoms, les fichiers, les bases de données …

Il n'est pas exclu cependant qu'une évaluation et une analyse des installations physiques (bâtiments, entrepôts …) ne soit pas nécessaire. Les services généraux évalueront pour leurs part les différents contrats des prestataires (assurance, hébergements, garanties, remplacement des serveurs et ordinateurs etc …).

Etape 6 : Rédiger un plan listant toutes les procédures définies.

Ce document devra être soumis et validé par la Direction Générale de l'Entreprise.

Il doit servir de base à :

- L'organisation des procédures définies.
- Identifier toutes les étapes majeures de mise en place du PRA.
- Proposer des solutions pour pallier aux manques identifiés.
- Envisager l'organisation la meilleure possible pour sécuriser le PRA.

Etape 7 : Définir les processus de test et de validation.

Cette étape devra aboutir à des procédures d'essai et de tests qui valideront au final le PRA.

Son objectif sera de :

- Valider la faisabilité du PRA, de vérifier les procédures et les installations de secours.
- Prévoir la formation du management et des collaborateurs.
- Identifier les points faibles éventuels du dispositif.
- Prévoir des tests et des mise à jour réguliers du PRA.

Etape 8 : Tester le PRA.

Une phase de tests est nécessaire pour valider tout ce qui aura été défini précédemment, que ce soit pour les procédures ou les solutions envisagées.

Pour cette étape, les scenarosi seront définies à partir des risques envisagés. Pour chaque risque on déroulera un scénario rédigé spécifiquement.

Etape 9 : Mise en route du PRA.

Une fois testé et validé par la Direction Générale, le PRA est mis en œuvre et évaluer/tester périodiquement.

10 Annexe 1 : Durée de conservation des documents.

Source : Service Public.fr

Type de document	Durée	Texte de référence
Documents Civils et Commerciaux		
Contrat ou convention conclu dans le cadre d'une relation commerciale, correspondance commerciale	5 ans	art. L.110-4 du code de commerce
Garantie pour les biens ou services fournis au consommateur	2 ans	art. L.137-2 du code de la consommation
Contrat conclu par voie électronique (à partir de 120 €)	10 ans à partir de la livraison ou de la prestation	art. L.134-2 du code de la consommation
Contrat d'acquisition ou de cession de biens immobiliers et fonciers	30 ans	art. 2227 du code civil
Document bancaire (talon de chèque, relevé bancaire...)	5 ans	art. L.110-4 du code de commerce
Document de transport de marchandises	5 ans	art. L.110-4 du code de commerce
Déclaration en douane	3 ans	art. 16 du règlement européen n°2913/92 du Conseil du 12 octobre 1992
Police d'assurance	2 ans à partir de la résiliation du contrat	art. L.114-1 du code des assurances
Document relatif à la propriété intellectuelle (dépôt de brevet, marque, dessin et modèle)	5 ans à partir de la fin de la protection	art. 2224 du code civil
Dossier d'un avocat	5 ans à partir de la fin du mandat	art. 2225 du code civil
Pièces Comptables		
Livre et registre comptable : livre journal, grand livre, livre d'inventaire...	10 ans à partir de la clôture de l'exercice	art. L.123-22 du code de commerce
Pièce justificative : bon de commande, de livraison ou de réception, facture client et fournisseur...	10 ans à partir de la clôture de l'exercice	art. L.123-22 du code de commerce
Documents fiscaux		
Impôt sur le revenu et sur les sociétés	6 ans	art. L.102 B du livre des procédures fiscales
Bénéfices industriels et commerciaux (BIC),	6 ans	art. L.102 B du livre des

Type de document	Durée	Texte de référence
bénéfices non commerciaux (BNC) et bénéfices agricoles (BA) en régime réel		procédures fiscales
Impôts sur les sociétés pour l'exercice, des sociétés à responsabilité limitée (exploitations agricoles, sociétés d'exercice libéral)	6 ans	art. L.102 B du livre des procédures fiscales
Impôts directs locaux (taxes foncières, contribution à l'audiovisuel public)	6 ans	art. L.102 B du livre des procédures fiscales
Cotisation foncière des entreprises (CFE)	6 ans	art. L.102 B du livre des procédures fiscales
Taxes sur le chiffre d'affaires (et taxes assimilées, impôt sur les spectacles, taxe sur les conventions d'assurance...)	6 ans	art. L.102 B du livre des procédures fiscales
Documents Sociaux (stés commerciales)		
Impôt sur le revenu et sur les sociétés	6 ans	art. L.102 B du livre des procédures fiscales
Bénéfices industriels et commerciaux (BIC), bénéfices non commerciaux (BNC) et bénéfices agricoles (BA) en régime réel	6 ans	art. L.102 B du livre des procédures fiscales
Impôts sur les sociétés pour l', des sociétés à responsabilité limitée (exploitations agricoles, sociétés d'exercice libéral)	6 ans	art. L.102 B du livre des procédures fiscales
Impôts directs locaux (taxes foncières, contribution à l'audiovisuel public)	6 ans	art. L.102 B du livre des procédures fiscales
Cotisation foncière des entreprises (CFE)	6 ans	art. L.102 B du livre des procédures fiscales
Taxes sur le chiffre d'affaires (et taxes assimilées, impôt sur les spectacles, taxe sur les conventions d'assurance...)	6 ans	art. L.102 B du livre des procédures fiscales
Gestion du personnel		
Bulletin de paie (double papier ou sous forme électronique)	5 ans	art. L.3243-4 du code du travail
Registre unique du personnel	5 ans à partir du départ du salarié	art. R.1221-26 du code du travail
Document concernant les contrats de travail, salaires, primes, indemnités, soldes de tout compte, régimes de retraite...	5 ans	art. 2224 du code civil

Type de document	Durée	Texte de référence
Document relatif aux charges sociales et à la taxe sur les salaires	3 ans	art. L.244-3 du code de la sécurité sociale et art. L.169 A du livre des procédures fiscales
Comptabilisation des jours de travail des salariés sous convention de forfait	3 ans	art. D.3171-16 du code du travail
Comptabilisation des horaires des salariés, des heures d'astreinte et de leur compensation	1 an	art. D.3171-16 du code du travail
Observation ou mise en demeure de l'inspection du travail	5 ans	art. D.4711-3 du code du travail
Déclaration d'accident du travail auprès de la caisse primaire d'assurance maladie	5 ans	art. D.4711-3 du code du travail

11 Annexe 2 : Glossaire de l'archivage électronique.

Archivage électronique
Ensemble des actions, outils et méthodes mis en oeuvre pour conserver àmoyen et à long terme des informations numériques dans le but de les rendre accessibles et exploitables. L'archivage électronique implique d'identifier précisément les responsabilités des différents acteurs (autorité juridique, autorité d'archivage...).

Archives courantes
Documents et données nécessaires à la gestion des affaires en cours et, comme tels, utilisés fréquemment par les services qui les ont produits.

Archives définitives
Documents et données conservés au-delà de leur durée d'utilité administrative, en raison de leur valeur patrimoniale (historique, statistique, scientifique) ou de leur intérêt public permanent.

Archives intermédiaires
Documents et données conservés à des fins de preuve même s'ils ne sont plus utilisés au quotidien.

Authenticité
Qualité d'un document ou d'une donnée dont l'origine, la réalité et l'auteur sont certifiés et incontestables. Dans le monde numérique, la signature électronique est un des procédés permettant de garantir cette qualité.

Cycle de vie des données/documents
Étapes que suit un document ou une donnée durant toute sa durée d'utilité administrative, de sa création jusqu'à la mise en oeuvre de son sort final.

Document d'activité
Informations créées, reçues et préservées comme preuves et actifs par une personne physique ou morale dans l'exercice de ses obligations légales ou la conduite de son activité.

Donnée
Représentation formalisée de l'information, adaptée à l'interprétation, au traitement et à la communication. La donnée est donc un conteneur porteur d'une information ou d'un fragment d'information.

Durée d'utilité administrative (DUA)
Durée de conservation d'un document nécessaire à la gestion des affaires en cours ou utile à des fins juridiques. La DUA de chaque document ainsi que son sort final sont rappelés dans les référentiels, les instructions de tri et les tableaux de gestion.

Empreinte
Terme de cryptologie désignant un ensemble de bits caractéristique d'un document numérique, obtenu par une fonction de hachage. Toute modification du document numérique entraîne une empreinte différente. La comparaison d'empreintes permet de contrôler l'intégrité d'un fichier.

Gestion électronique des documents (GED)
Outil informatique permettant d'organiser et de gérer des documents ou données électroniques au sein d'un organisme et recouvrant des fonctionnalités de capture et de contrôle des données et des documents, de gestion des versions et des métadonnées, de recherche et des modules de contrôle des circuits de validation des documents.

Informatique en nuage (cloud computing)
Mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire. L'informatique en nuage est une forme particulière de gérance de l'informatique, dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des clients. Elle se caractérise par un accès à des ressources informatiques à la demande via un réseau à large bande (généralement internet), une mutualisation des ressources, une adaptabilité rapide et par un service mesuré et facturé à l'usage.

Métadonnées
Ensemble structuré d'informations techniques, de gestion et de description attachées à un document servant à décrire les caractéristiques de ce document en vue de faciliter son repérage, sa gestion, son usage ou sa préservation.

Signature électronique
Mécanisme qui permet l'identification de l'auteur d'un document électronique, la garantie de l'intégrité de ce document et le lien entre le document et la signature.

Sort final
Décision de conservation (totale ou partielle) ou d'élimination de documents ou de données mise en oeuvre à l'issue de la DUA.

Système d'archivage électronique (SAE)
Ensemble d'infrastructures matérielles et logicielles permettant de conserver et de restituer des documents ou données électroniques sur le long terme en garantissant leur intégrité et leur lisibilité.

Tiers-archiveur
Personne qui se charge, pour le compte de tiers, d'assurer et de garantir la conservation et l'intégrité d'archives
publiques courantes ou intermédiaires, sur support papier ou numérique.